最近有很多小伙伴咨询关于proofofwork的问题，小编结合多年的经验整理出来一些proofofwork的缺点有以下哪几项对应的资料，分享给大家。

PoC的本质，用一个普通人也可以理解的话说，就是用硬盘挖矿。没错，PoW是用CPU（或者显卡、ASIC矿机，他们的本质都是更强的计算芯片，与CPU本质上是一样的）挖矿、PoS是凭借持币比例挖矿，DPoS是根据投票决定超级节点，而PoC就是凭借硬盘挖矿。

我们可以这么理解：

-在PoW里是谁的芯片计算快、谁就容易挖到矿；

-在PoS里是谁持币多，谁就容易挖到矿；

-在DPoS里是谁获得的投票多，谁就能成为超级节点进行挖矿；

-在PoC里就是谁的硬盘容量大，谁就容易挖到矿。

是不是足够简单易懂了吧！

要理解PoC的具体原理，我们还是得从比特币PoW入手（研究区块链，PoW就是你永远也绕不过去的技术概念）。

PoW的全称是Proof of Work，即工作量证明。这儿所谓的工作量，就是矿工的CPU（或者显卡、ASIC芯片，我们前面已经说过，这些硬件只是计算速度更快，本质和CPU并无区别）执行一种叫做哈希算法的计算工作。简而言之，谁能够在单位时间内执行更多次的哈希计算，谁就有更大几率产生一个符合要求的哈希结果、进而拿到写入区块链的权利。

可以这么说，比特币PoW的本质就是算力竞争挖矿。每一个新区块的产生，就是给矿工出一道“难题”，矿工通过算力竞争，比拼谁能够先找到符合要求的“答案”。矿工通过购买牛逼的计算芯片，以及持续地消耗电能进行高频率高强度的哈希计算，去获得更强的算力占比，进而获得更大的找到“答案”的概率。如果一个比特币矿工拥有全网20%的算力，理论上他就可以挖出20%的新区块、进而获得20%的区块奖励（最早每个块有50个比特币奖励，现在已经减少到12.5个，明年还会继续减半）。

PoW挖矿规则简单粗暴、算力可以自由进出，因此能建立足够的安全性，来保证区块链不被篡改的特性。这就是为什么比特币虽然技术看似简单，但是能够成为币王

之王，占据一半左右的市值。

此外，比特币的分叉币（例如BCH和BSV）、莱特币LTC、以太坊ETH、门罗币Monero、达世币Dash也都是全部或部分采用了PoW机制挖矿的币种，只不过这些币种可能在一些技术参数上与比特币有区别，但总体思想是类似的。

我们今天的主角PoC，和比特币PoW有异曲同工之妙，但是又有一些实质性的区别。我们知道，比特币PoW要求矿工持续地、反复地执行哈希计算，矿工需要高强度地运行他们的计算芯片，并消耗极为可观的电力资源。

我们的PoC则是另行开辟了一条极为巧妙的道路：它要求矿工预先计算好数量巨大的哈希结果，并将这些数据存储在硬盘里；挖矿的时候，矿工也是争相破解“难题”，不同的是“难题”的答案要在硬盘数据中找，而不是实时地计算。自然而然，谁的硬盘容量更大，谁就有能预先存储更多的“备选答案”，谁就有更高的概率找到能够匹配“难题”的那个“正确答案”。

有人可能要问了，在PoC这个机制中，矿工有没有可能通过芯片去计算答案作弊呢？不可能。PoC的算法设计决定了它在找“答案”的时候，对存储空间这一要素非常敏感，而对芯片的计算能力不那么敏感。强大的算力对矿工挖矿成功率加成并不是很大，而拥有更多的存储空间倒是能成倍地提高挖矿成功率。PoC的这种特性也被形象地称为“空间换时间”。

POW是Proof Of Work的简称，中文翻译是工作量证明，是一种去中心化的，公开透明的，不可篡改的算法机制。比特币就是采用POW共识算法，10年运行安全平稳。目前以太经典（ETC）也是采用这种算法机制，通过算力挖矿可以获得奖励。

detailed

proof

直接翻译是“详细证明”。

relavant

work

experience

是指相关工作经验。所以要写出之前曾经做过什么相关的行业，最好能写出对工作

的熟悉度。

ProofofWork的优点：

1、机制本身当然很复杂，有很多细节，比如：挖矿难度自动调整、区块奖励逐步减半等，这些因素都是基于经济学原理，能吸引和鼓励更多人参与。

2、理想状态，这种机制，可以吸引很多用户参与其中，特别是越先参与的获得越多，会促使加密货币的初始阶段发展迅速，节点网络迅速扩大。在Cpu挖矿的时代，比特币吸引了很多人参与“挖矿”，就是很好的证明。

3、通过“挖矿”的方式发行新币，把比特币分散给个人，实现了相对公平。

缺点：

1、算力是计算机硬件（Cpu、Gpu等）提供的，要耗费电力，是对能源的直接消耗，与人类追求节能、清洁、环保的理念相悖。不过，如果非要给“加密货币”找寻“货币价值”的意义，那么这个方面，应该是最有力的证据。

2、这种机制发展到今天，算力的提供已经不再是单纯的CPU了，而是逐步发展到GPU、FPGA，乃至ASIC矿机。用户也从个人挖矿发展到大的矿池、矿场，算力集中越来越明显。这与去中心化的方向背道而驰，渐行渐远，网络的安全逐渐受到威胁。有证据证明Ghash（一个矿池）就曾经对赌博网站实施了双花攻击（简单的说就是一笔钱花两次）。

3、比特币区块奖励每4年将减半，当挖矿的成本高于挖矿收益时，人们挖矿的积极性降低，会有大量算力减少，比特币网络的安全性进一步堪忧。

PoC是Proof of Capacity的缩写，翻译成汉语就是容量证明。顾名思义，就是通过存储容量的多少来决定区块生成权的算法。PoC共识机制用更加通俗的语言表达就是用CPU，GPU预算出一堆彩票号码，然后填满硬盘，挖矿就是寻找中奖的彩票号码。

目前大部分数字货币挖矿采用的是PoW（工作量证明）。仅有Burst、BHD、Newbi使用PoC共识机制。

proof of work

工作证明

双语例句

proof of work

工作量证明

proofofwork是很多人头疼的问题，尤其是在理解和现实的冲突方面，proofofwork的缺点有以下哪几项也同样面临着相似的问题，关注我们，为您服务，是我们的荣幸！